TABLA DE CONTENIDO

INTRODUCCIÓN 2

OBJETIVO 3

OBJETIVO GENERAL 3
OBJETIVOS ESPECÍFICOS 3

ALCANCE 3

MARCO NORMATIVO Y DE REFERENCIA 5

PRINCIPIOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6

JUSTIFICACIÓN Y ARTICULACIÓN CON EL MIPG Y EL PLAN ESTRATÉGICO INSTITUCIONAL (PEI) 8

GLOSARIO Y TÉRMINOS DE REFERENCIA 9

CONTEXTO ESTRATÉGICO Y PARTES INTERESADAS 11

DIAGNÓSTICO DE MADUREZ EN SEGURIDAD DIGITAL (AUTODIAGNÓSTICO MSPI) 12

INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 14

GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 15

PLAN DE TRATAMIENTO DE RIESGOS 17

DIRECTRICES GENERALES DEL MSPI 18

ROLES Y RESPONSABILIDADES 20

GOBERNANZA Y TRES LÍNEAS DE DEFENSA 21

RELACIÓN CON PROVEEDORES Y SERVICIOS EN LA NUBE 22

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 24

CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES 25

SOSTENIBILIDAD DIGITAL Y GESTIÓN AMBIENTAL DE TIC 26

PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD 27

SERVICIOS CIUDADANOS DIGITALES Y TRANSPARENCIA 29

CAPACITACIÓN Y CULTURA ORGANIZACIONAL EN SEGURIDAD DIGITAL 31

INDICADORES DE SEGUIMIENTO Y EVALUACIÓN 32

SEGUIMIENTO, ARTICULACIÓN CON AUDITORÍAS INTERNAS Y EXTERNAS, E INDICADORES DE EVALUACIÓN 33

VERIFICACIÓN, REVISIÓN Y ACTUALIZACIÓN DEL MSPI 35

DISPOSICIONES FINALES 36

Introducción

El Modelo de Seguridad y Privacidad de la Información (MSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) constituye el marco institucional para gestionar de manera integral la seguridad digital, proteger los activos de información y garantizar la prestación continua y confiable de los servicios públicos domiciliarios.

Este documento define los lineamientos, procesos y controles que permiten administrar la confidencialidad, integridad, disponibilidad y privacidad (CIDP) de la información, en cumplimiento de la normatividad nacional vigente, los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas internacionales en ciberseguridad.

El modelo se fundamenta en la Resolución MinTIC 500 de 2021 y en sus actualizaciones, en particular la Resolución 2277 de 2025, que establecen la obligatoriedad de implementar y fortalecer el MSPI en las entidades públicas. Asimismo, incorpora la Estrategia Nacional de Confianza y Seguridad Digital 2025–2027, el Decreto 338 de 2022 sobre Gobierno Digital, y lo dispuesto en las leyes relacionadas con delitos informáticos, protección de datos personales, transparencia y gestión documental.

Como referentes técnicos, EPC adopta estándares internacionales tales como ISO/IEC 27001:2022, ISO/IEC 27002, ISO/IEC 27005, ISO 22301:2019 y el NIST Cybersecurity Framework 2.0, los cuales orientan la implementación de controles, la gestión de riesgos, la continuidad de negocio y la respuesta ante incidentes.

La construcción de este modelo se apoya en los resultados del autodiagnóstico MSPI, en el inventario institucional de activos de información, en el mapa de riesgos TI, y en los planes estratégicos de la entidad, particularmente el PETI y el PESI, estos insumos garantizan que la gestión de la seguridad digital esté integrada a la planeación institucional, al MIPG y al Sistema Integrado de Gestión.

Finalmente, el MSPI incorpora un enfoque de mejora continua mediante el ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando auditorías internas, revisiones por la dirección, resultados de control interno y el reporte al FURAG, con este modelo, EPC reafirma su compromiso con la confianza ciudadana, la

transparencia, la protección de datos personales y la sostenibilidad digital en el marco de la transformación digital del sector público.

Objetivo

Objetivo General

Establecer el modelo de gestión integral de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), que permita proteger los activos institucionales, garantizar la confidencialidad, integridad, disponibilidad y privacidad (CIDP) de la información, y asegurar la continuidad de los servicios tecnológicos y misionales, en cumplimiento de la normatividad nacional y los lineamientos del MinTIC, con base en estándares internacionales de referencia.

Objetivos Específicos

- Implementar un sistema de gestión de la seguridad de la información alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI), integrando políticas, procedimientos, controles y buenas prácticas de ciberseguridad en todos los procesos institucionales.
- Desarrollar un esquema de gestión de riesgos que permita identificar, analizar, valorar, tratar y monitorear los riesgos de seguridad digital, en coherencia con el Mapa de Riesgos Institucionales, el Plan de Tratamiento de Riesgos y la metodología establecida en la ISO/IEC 27005.
- Promover una cultura organizacional de seguridad digital mediante la sensibilización, formación y compromiso de funcionarios, contratistas y proveedores, asegurando el cumplimiento de la Ley 1581 de 2012, la Ley 1712 de 2014, la Ley 1273 de 2009, el Decreto 338 de 2022 y demás normatividad aplicable, en articulación con el MIPG y el Sistema Integrado de Gestión.

Alcance

El Modelo aplica a todos los procesos, áreas, funcionarios, contratistas, proveedores y terceros que gestionen, accedan o administren información y recursos tecnológicos de la entidad. Su cobertura es transversal e institucional, y constituye un marco obligatorio de cumplimiento.

El alcance comprende las siguientes dimensiones:

- **Activos de información**: incluye la identificación, clasificación, valoración y protección de los activos físicos, digitales y tecnológicos registrados en el Inventario Institucional de Activos de Información, considerando su criticidad en términos de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
- **Infraestructura tecnológica**: abarca equipos de cómputo, servidores, redes de telecomunicaciones, sistemas de almacenamiento, servicios en la nube, aplicaciones y bases de datos que soportan los procesos misionales y de apoyo de EPC.
- **Gestión de riesgos**: integra la identificación, análisis, tratamiento y monitoreo de riesgos relacionados con la seguridad y privacidad de la información, en coherencia con la ISO/IEC 27005, el Mapa de Riesgos Institucionales y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- **Controles de seguridad**: comprende la definición e implementación de controles técnicos (cifrado, autenticación multifactor, SIEM, respaldos), organizacionales (políticas, roles y procedimientos), contractuales (cláusulas de seguridad y continuidad) y operativos (monitoreo, continuidad y recuperación).
- **Relación con terceros**: cubre la interacción con proveedores y aliados estratégicos que presten servicios tecnológicos, quienes deberán cumplir con las cláusulas contractuales y con los lineamientos del MinTIC en materia de seguridad digital y servicios en la nube.
- **Gestión de incidentes**: incluye la detección, reporte, análisis, respuesta y cierre de incidentes de seguridad de la información, así como la documentación y lecciones aprendidas.
- **Continuidad del negocio y recuperación ante desastres**: asegura la ejecución de planes de continuidad y recuperación de servicios críticos en cumplimiento de la ISO 22301:2019 y el Decreto 2157 de 2017, minimizando impactos en la operación institucional.
- **Protección de datos personales**: garantiza la aplicación de la Ley 1581 de 2012 y su reglamentación, mediante el cumplimiento de principios y medidas técnicas, jurídicas y organizacionales orientadas a salvaguardar los derechos de los titulares de la información.
- **Gobierno digital y transparencia**: articula el MSPI con la Política de Gobierno Digital, los Servicios Ciudadanos Digitales y las disposiciones de la Ley 1712 de 2014, asegurando la confianza ciudadana en el manejo de la información pública.

En conclusión, el MSPI se aplica a todo el ecosistema de información y tecnología de EPC, garantizando que la seguridad digital sea un eje transversal en la planeación institucional, la prestación de servicios públicos y la gestión con partes interesadas.

Marco Normativo y de Referencia

El Modelo de Seguridad y Privacidad de la Información (MSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) se fundamenta en la normatividad nacional vigente, los lineamientos expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en marcos internacionales de referencia en ciberseguridad y gestión de riesgos.

Normatividad nacional aplicable

- Ley 1273 de 2009: tipifica los delitos informáticos y la protección de la información y de los datos.
- Ley 1581 de 2012 y Decreto 1377 de 2013: regulan la protección de datos personales y los derechos de los titulares.
- Ley 1712 de 2014 y Decreto 103 de 2015: establecen el derecho de acceso a la información pública y la transparencia.
- Ley 594 de 2000: Ley General de Archivos, que regula la función archivística del Estado.
- Decreto 1008 de 2018 y Decreto 338 de 2022: regulan la Política de Gobierno Digital y sus lineamientos.
- Decreto 2157 de 2017: reglamenta la gestión de continuidad de negocio en entidades públicas y privadas.
- Resolución MinTIC 500 de 2021, Resolución 2277 de 2025 y Resolución 1236 de 2025: lineamientos obligatorios para la implementación y fortalecimiento del MSPI.
- Conpes 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- Estrategia Nacional de Confianza y Seguridad Digital 2025–2027: hoja de ruta vigente para fortalecer la seguridad digital, la resiliencia cibernética y la coordinación interinstitucional en Colombia.

Normatividad institucional de referencia

- Política General de Seguridad de la Información.
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Plan Estratégico de Tecnologías de la Información (PETI).

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Mapa de Riesgos de Gestión y Corrupción – TI.
- Plan de Contingencia y Recuperación en Seguridad Informática.
- Inventario y Clasificación de Activos de Información.
- Matriz de Contexto Estratégico – Gestión de TI.
- Matriz de Partes Interesadas – Área de TI.
- Normograma de Gestión de TI.

Marcos y estándares internacionales de referencia

- ISO/IEC 27001:2022: sistemas de gestión de seguridad de la información.
- ISO/IEC 27002:2022: controles de seguridad de la información.
- ISO/IEC 27005: gestión de riesgos de seguridad de la información.
- ISO/IEC 27017 y 27018: seguridad y privacidad en servicios de nube.
- ISO/IEC 27031:2025: continuidad de negocio en entornos de TI.
- ISO 22301:2019: sistemas de gestión de continuidad de negocio.
- ISO 31000:2018: gestión del riesgo.
- ISO/IEC 27035: gestión de incidentes de seguridad de la información.
- NIST Cybersecurity Framework 2.0: gestión de riesgos de ciberseguridad.
- COBIT 2019: gobernanza y gestión de TI.

Este marco normativo y de referencia asegura que el MSPI de EPC se ejecute bajo un enfoque integral, cumpliendo las disposiciones nacionales, los lineamientos del MinTIC y las mejores prácticas internacionales, garantizando trazabilidad, seguridad y resiliencia digital en todos los procesos institucionales.

Principios del Modelo de Seguridad y Privacidad de la Información

Se rige por principios que orientan la gestión integral de la seguridad digital y garantizan que las acciones de protección se ejecuten de manera coherente, técnica y sostenible.

Confidencialidad

La información debe estar protegida frente a accesos no autorizados, divulgación indebida o uso inadecuado, este principio se asegura mediante la implementación de controles de acceso basados en el principio de mínimo privilegio, autenticación multifactor, cifrado de datos y acuerdos de confidencialidad con funcionarios, contratistas y proveedores.

Integridad
Los datos deben mantenerse exactos, consistentes y libres de alteraciones no autorizadas, la integridad se protege a través de la gestión de cambios, controles de versionamiento, uso de firmas digitales, trazabilidad de registros y mecanismos de auditoría.

Disponibilidad
La información, sistemas y servicios tecnológicos deben estar accesibles de manera oportuna para los usuarios autorizados, se garantiza con planes de continuidad del negocio, redundancia en infraestructuras críticas, respaldos periódicos, recuperación ante desastres y acuerdos de niveles de servicio (SLA) con proveedores estratégicos.

Privacidad
El tratamiento de datos personales se realiza en cumplimiento estricto de la Ley 1581 de 2012 y sus decretos reglamentarios, asegurando la protección de los derechos de los titulares, se aplican medidas como anonimización de datos, control de autorizaciones, gestión de incidentes relacionados con privacidad y auditorías periódicas de cumplimiento.

Cumplimiento normativo

Todas las actividades del MSPI deben observar las leyes nacionales, lineamientos del MinTIC y estándares internacionales aplicables. El cumplimiento se valida a través de auditorías internas, evaluaciones de control, revisiones por la dirección y la aplicación anual del autodiagnóstico MSPI.

Gestión de riesgos

La seguridad de la información se administra bajo un enfoque de riesgos, identificando amenazas, vulnerabilidades y probabilidad de ocurrencia, en alineación con la ISO/IEC 27005 y con el Mapa de Riesgos Institucionales. El tratamiento se enfoca en proteger los activos críticos y garantizar la resiliencia organizacional.

Responsabilidad compartida

La seguridad digital no es exclusiva del área de TI. Todos los funcionarios, contratistas y terceros con acceso a los activos de información son responsables de aplicar buenas prácticas, cumplir las políticas y reportar incidentes oportunamente.

Mejora continua

El MSPI se fortalece permanentemente mediante la aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar), incorporando resultados del autodiagnóstico, auditorías internas, revisiones de la dirección, hallazgos de control interno y lineamientos actualizados del MinTIC.

Transparencia y confianza ciudadana

La apertura de datos y la provisión de servicios digitales deben ejecutarse con esquemas de seguridad que fortalezcan la confianza en la gestión pública, en cumplimiento de la Ley 1712 de 2014 y de la Política de Gobierno Digital.

Sostenibilidad digital

La seguridad de la información incorpora prácticas responsables con el medio ambiente, tales como la reducción del consumo de papel, la disposición adecuada de residuos electrónicos (RAEE), el uso eficiente de la infraestructura tecnológica y el fomento del teletrabajo, en consonancia con los Objetivos de Desarrollo Sostenible (ODS).

Justificación y Articulación con el MIPG y el Plan Estratégico Institucional (PEI)

Su implementación asegura que la seguridad digital no sea tratada como un proceso aislado de carácter técnico, sino como un componente transversal de la planeación, la gestión institucional y la toma de decisiones, con impacto directo en la confianza ciudadana y en la continuidad de la prestación de los servicios públicos.

La adopción del MSPI responde a la necesidad de dar cumplimiento a la normatividad vigente en materia de Gobierno Digital y seguridad de la información, en particular el Decreto 338 de 2022, la Política de Gobierno Digital, el Conpes 4070 de 2021 – Política Nacional de Confianza y Seguridad Digital, la Ley 1581 de 2012 de protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, así como a los lineamientos de la Guía de Riesgos del DAFP y el FURAG, además, articula su gestión con estándares internacionales como ISO/IEC 27001, 27005, 27017 y 27018, el NIST CSF 2.0 y el COBIT 2019, que constituyen marcos de referencia reconocidos a nivel global.

En términos de gobernanza, el MSPI se encuentra alineado con el Modelo Integrado de Planeación y Gestión (MIPG), integrando su ciclo de gestión con los pilares de planeación, ejecución, seguimiento y evaluación, esta articulación asegura que los riesgos de seguridad de la información se identifiquen, valoren y gestionen en coherencia con los objetivos estratégicos de la entidad y con las políticas públicas nacionales. En este sentido, los resultados del autodiagnóstico MSPI, los reportes de auditoría y las matrices de riesgos se convierten en insumos para el proceso de revisión por la dirección y para la definición de acciones de mejora continua.

El MSPI también mantiene una relación directa con el Plan Estratégico Institucional (PEI), dado que contribuye al cumplimiento de los objetivos misionales mediante la protección de la información, la continuidad operativa y la confianza digital, esta articulación se materializa en la integración del modelo con el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), garantizando que la seguridad de la información esté incorporada en todos los proyectos tecnológicos, en la modernización institucional y en el fortalecimiento de los servicios ciudadanos digitales.

De esta manera, el MSPI se justifica como una herramienta indispensable para EPC, no solo porque asegura la confidencialidad, integridad, disponibilidad y privacidad de la información, sino porque también garantiza la alineación con los lineamientos del MIPG y la coherencia con el PEI, consolidando un ecosistema de gestión pública más seguro, transparente, confiable y orientado a resultados.

Glosario y Términos de Referencia

Activo de información: Recurso, dato, documento, aplicación, sistema, infraestructura tecnológica o servicio que tiene valor para la entidad y que debe ser protegido frente a amenazas que afecten su confidencialidad, integridad, disponibilidad o privacidad.
CIDP (Confidencialidad, Integridad, Disponibilidad y Privacidad): Principios fundamentales de la seguridad de la información que orientan el diseño e implementación de controles y estrategias de protección.
Continuidad de negocio (BCP – Business Continuity Planning): Capacidad de la entidad para mantener sus funciones críticas y servicios esenciales en niveles aceptables, durante y después de incidentes graves o desastres, mediante planes, procedimientos y medidas de resiliencia.

Control de seguridad: Medida técnica, organizacional, contractual u operativa implementada para reducir la probabilidad o el impacto de un riesgo sobre los activos de información.
FURAG (Formulario Único de Reporte de Avances de la Gestión): Instrumento definido por el Departamento Administrativo de la Función Pública que permite a las entidades públicas reportar los avances en la implementación del MIPG y del MSPI.
Gobierno Digital: Política pública definida en el Decreto 338 de 2022, orientada a promover la transformación digital del Estado, los Servicios Ciudadanos Digitales, la apertura de datos y la seguridad digital.
ICC (Infraestructura Crítica Cibernética): Conjunto de activos tecnológicos y de información cuya afectación comprometería de manera grave la prestación de servicios públicos, la seguridad ciudadana o la estabilidad institucional.
Incidente de seguridad de la información: Evento que afecta o puede afectar la confidencialidad, integridad, disponibilidad o privacidad de la información o de los sistemas tecnológicos, incluyendo accesos no autorizados, malware, pérdida de datos, ataques cibernéticos o fallas críticas.
MSPI (Modelo de Seguridad y Privacidad de la Información): Modelo definido por el MinTIC y adoptado en las entidades públicas, que establece los lineamientos y controles para la gestión integral de la seguridad digital en Colombia.
Nube (Cloud Computing): Modelo de prestación de servicios tecnológicos a través de internet, que permite acceso bajo demanda a recursos informáticos compartidos. En el MSPI, su uso está regulado por la ISO/IEC 27017 y la ISO/IEC 27018, además de las directrices del MinTIC.
PETI (Plan Estratégico de Tecnologías de la Información): Instrumento de planeación que define los objetivos, proyectos y acciones estratégicas de TI para garantizar la modernización tecnológica y la prestación eficiente de servicios institucionales.
PESI (Plan Estratégico de Seguridad y Privacidad de la Información): Documento estratégico que operacionaliza la política de seguridad de la información y define los programas, controles y acciones para implementar el MSPI en la entidad.
RAEE (Residuos de Aparatos Eléctricos y Electrónicos): Equipos en desuso que requieren un manejo ambientalmente responsable para mitigar riesgos ambientales y sanitarios, y que forman parte de la sostenibilidad digital de la entidad.
SIEM (Security Information and Event Management): Plataforma tecnológica para la centralización, monitoreo, correlación y análisis de eventos de

seguridad, que permite detectar amenazas en tiempo real y mejorar la capacidad de respuesta institucional.
Usuario final: funcionario, contratista o tercero autorizado para acceder, consultar o administrar información institucional en el marco de sus funciones o actividades contractuales.

Contexto Estratégico y Partes Interesadas

La implementación se desarrolla en un entorno institucional, normativo y tecnológico que demanda fortalecer la seguridad digital como un eje estratégico de la gestión pública.

Contexto estratégico

EPC, como entidad prestadora de servicios públicos, administra información sensible relacionada con usuarios, operaciones técnicas, proyectos de infraestructura y gestión administrativa, en este escenario, los riesgos asociados a la pérdida, alteración o divulgación indebida de información pueden afectar la continuidad de los servicios, la confianza ciudadana y el cumplimiento de los objetivos misionales.

El MSPI se articula con:

- El Plan Estratégico Institucional (PEI), que define los lineamientos de mediano plazo para la entidad.
- El Plan Estratégico de Tecnologías de la Información (PETI), que establece los proyectos tecnológicos prioritarios.
- El Plan Estratégico de Seguridad y Privacidad de la Información (PESI), que operacionaliza las medidas de seguridad digital.
- El Mapa de Riesgos Institucionales y de TI, que identifica amenazas y vulnerabilidades críticas.
- El MIPG y los compromisos reportados en el FURAG, que garantizan el alineamiento con las políticas de gestión pública.

Partes interesadas

La seguridad digital de EPC debe responder a las expectativas y necesidades de los actores internos y externos con quienes la entidad interactúa de manera directa:

- Administraciones municipales: demandan información segura y confiable para coordinar acciones en el territorio.

- Gobernación de Cundinamarca: requiere articulación técnica y estratégica en proyectos departamentales.
- Prestadores de servicios públicos: necesitan interoperabilidad segura en el intercambio de datos y procesos.
- Entes de control: exigen cumplimiento normativo, evidencia de gestión y trazabilidad en las acciones de seguridad.
- Gobierno Nacional y entidades gubernamentales: requieren alineación con la Política de Gobierno Digital, el MSPI y la Estrategia Nacional de Confianza y Seguridad Digital.
- Junta Directiva: demanda información confiable para la toma de decisiones estratégicas.
- Comité Directivo del Plan Departamental de Aguas (PDA): exige controles adecuados en el manejo de datos y sistemas de información relacionados con los proyectos de agua y saneamiento.
- Medios de comunicación: requieren acceso oportuno y seguro a la información institucional de carácter público.
- Ciudadanos: esperan transparencia, acceso confiable a la información y protección de sus datos personales.
- Contratistas y proveedores: deben cumplir con cláusulas contractuales de seguridad digital y garantizar continuidad en los servicios tecnológicos.
- Veedurías ciudadanas y asociaciones de usuarios: demandan trazabilidad y apertura de datos bajo principios de seguridad y privacidad.
- Colaboradores (funcionarios y contratistas internos): necesitan lineamientos claros para el manejo responsable de la información.
- Empresas privadas y comunidades educativas: requieren canales seguros de colaboración y transferencia de conocimiento.

La identificación del contexto estratégico y de las partes interesadas permite alinear el MSPI con los objetivos institucionales de EPC, reforzar la confianza de los ciudadanos y asegurar el cumplimiento de las obligaciones legales, contractuales y misionales de la entidad.

Diagnóstico de Madurez en Seguridad Digital (Autodiagnóstico MSPI)

El nivel de madurez fue evaluado mediante la aplicación del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), en cumplimiento de la Resolución MinTIC 2277 de 2025.

Resultado de madurez

De acuerdo con la última medición, EPC alcanzó un nivel de madurez 2 – Definido, con un puntaje del 48 %. Esto significa que la entidad cuenta con políticas, procesos y controles formalmente establecidos en materia de seguridad y privacidad de la información, aunque aún existen oportunidades de mejora para consolidar un nivel de gestión más robusto y sostenible.

Hallazgos principales

- Se cuenta con una Política General de Seguridad de la Información y un Plan Estratégico de Seguridad y Privacidad de la Información (PESI) actualizados y articulados con el PETI.
- El Inventario de Activos de Información está consolidado, aunque requiere mayor fortalecimiento en la clasificación por criticidad y trazabilidad con riesgos específicos.
- Existen controles técnicos implementados (respaldos, firewall, antivirus, autenticación multifactor), pero se requiere avanzar en la adopción de herramientas de monitoreo centralizado como SIEM y en la gestión sistemática de vulnerabilidades.
- Los procedimientos de gestión de incidentes se encuentran definidos, pero deben complementarse con simulacros anuales y con protocolos de comunicación hacia partes interesadas.
- Se han realizado capacitaciones en seguridad digital, aunque la cobertura debe ampliarse a todos los funcionarios, contratistas y proveedores tecnológicos.
- El proceso de gestión de riesgos se encuentra en operación, pero es necesario reforzar la integración con el Mapa de Riesgos Institucional y los informes de seguimiento al control interno.

Oportunidades de mejora identificadas

- Fortalecer la continuidad del negocio mediante pruebas periódicas de recuperación y redundancia en servicios críticos.
- Integrar cláusulas de seguridad más detalladas en los contratos tecnológicos y mejorar la supervisión a proveedores.
- Incrementar la cultura institucional en seguridad digital mediante campañas periódicas, boletines y programas de sensibilización.
- Potenciar los mecanismos de auditoría y seguimiento con indicadores más específicos (tiempo promedio de atención a incidentes, porcentaje de incidentes cerrados, porcentaje de activos críticos con controles aplicados).

El diagnóstico de madurez constituye la base para la implementación de las directrices del MSPI, y será evaluado de forma anual y de manera extraordinaria cuando se presenten cambios normativos, incidentes críticos o transformaciones tecnológicas de alto impacto.

Inventario y Clasificación de Activos de Información

La protección de la información institucional parte de una adecuada identificación, clasificación y gestión de los activos que la componen, mantieniendo un Inventario Institucional de Activos de Información, el cual constituye la base para la aplicación de controles, la gestión de riesgos y la continuidad de negocio.

Tipos de activos inventariados

- Información: documentos físicos y electrónicos, bases de datos, reportes, expedientes, comunicaciones oficiales.
- Tecnológicos: hardware, software, aplicaciones, sistemas de información, servicios en la nube, redes y telecomunicaciones.
- Servicios: sistemas críticos de operación, plataformas de soporte institucional y de atención ciudadana.
- Talento humano: funcionarios, contratistas y terceros que interactúan con los activos de información en el marco de sus funciones.

Clasificación por criticidad

Los activos se valoran con base en los principios de confidencialidad, integridad, disponibilidad y privacidad (CIDP), determinando un nivel de criticidad:

- Alta criticidad: su afectación comprometería la prestación de servicios públicos, la continuidad de negocio o el cumplimiento de obligaciones legales.
- Media criticidad: su afectación impactaría procesos internos, generando retrasos o reprocesos, aunque con capacidad de recuperación.
- Baja criticidad: activos de apoyo cuya afectación tendría un impacto limitado y de fácil recuperación.

Relación con riesgos y controles

Cada activo debe estar vinculado a:

- Amenazas y vulnerabilidades identificadas en el Mapa de Riesgos de TI.
- Medidas de mitigación documentadas en el Plan de Tratamiento de Riesgos.
- Controles existentes (técnicos, organizacionales y contractuales).

Responsabilidades

- El Coordinador TI es responsable de administrar el inventario, definir criterios de clasificación y coordinar la protección de activos críticos.
- La Mesa de Ayuda (MDA) registra, actualiza y monitorea los activos, reportando cambios o incidencias.
- Los propietarios de la información deben asegurar el uso adecuado y cumplir con los controles aplicables.

Revisión y actualización

El inventario será revisado y actualizado anualmente, o de manera extraordinaria cuando:

- Se adquieran o implementen nuevos sistemas o servicios tecnológicos.
- Se presenten incidentes de seguridad que afecten la clasificación de activos.
- Exista cambio normativo o auditoría que exija su actualización.

El Inventario y Clasificación de Activos de Información es un insumo transversal para el autodiagnóstico MSPI, la gestión de riesgos, el PETI y el PESI, garantizando que la seguridad digital esté orientada a proteger lo que tiene mayor valor para la entidad y la ciudadanía.

Gestión de Riesgos de Seguridad y Privacidad de la Información

La gestión de riesgos constituye un componente esencial, orientado a identificar, analizar, valorar, tratar y monitorear los riesgos que puedan afectar la seguridad digital y la continuidad de los servicios de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC).

Metodología aplicada

La entidad adopta la metodología establecida en la ISO/IEC 27005, complementada con los lineamientos de la ISO 31000:2018 y la normatividad nacional en materia de gestión de riesgos, esta metodología se articula con el Mapa de Riesgos Institucionales y con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Etapas de la gestión de riesgos

- Identificación: se determinan amenazas internas y externas, vulnerabilidades y activos expuestos, incluyendo riesgos tecnológicos, organizacionales, regulatorios y ambientales.

- Análisis: se evalúan la probabilidad de ocurrencia y el impacto potencial, considerando consecuencias operativas, financieras, legales y reputacionales.
- Valoración: se establece el nivel de riesgo inherente y residual, clasificándolo en zonas de riesgo (alto, medio o bajo).
- Tratamiento: se definen opciones de manejo, que pueden ser mitigar, transferir, aceptar o eliminar el riesgo.
- Monitoreo y revisión: se realiza seguimiento continuo a los riesgos identificados, a los controles aplicados y a los riesgos emergentes.

Categorías de riesgos gestionados

- Tecnológicos: fallas de hardware o software, interrupciones de telecomunicaciones, ataques cibernéticos, explotación de vulnerabilidades.
- Organizacionales: errores humanos, falta de capacitación, procesos ineficientes, incumplimiento de procedimientos.
- Exógenos: desastres naturales, interrupción de proveedores estratégicos, crisis sanitarias, fraudes externos.
- Jurídicos y regulatorios: incumplimiento de la Ley 1581 de 2012 (protección de datos), Ley 1712 de 2014 (transparencia), Decreto 338 de 2022 (Gobierno Digital), entre otros.

Responsables

- El Coordinador TI lidera la gestión de riesgos y coordina la integración con los sistemas institucionales de control.
- La Mesa de Ayuda (MDA) apoya en la recolección de información, el monitoreo y el registro de incidentes relacionados con riesgos identificados.
- El Comité de Gestión y Desempeño Institucional revisa y aprueba los resultados de la gestión de riesgos y define acciones estratégicas.
- Control Interno verifica la efectividad de las medidas y reporta hallazgos a los órganos de control.

Articulación con otros instrumentos

Los resultados de la gestión de riesgos alimentan directamente:

- El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- El PESI y el PETI, asegurando coherencia entre seguridad digital y planeación institucional.
- Los reportes al FURAG y a los entes de control.

La gestión de riesgos permite a EPC anticiparse a amenazas, reducir vulnerabilidades, proteger activos críticos y fortalecer su resiliencia institucional frente a incidentes y cambios en el entorno tecnológico.

Plan de Tratamiento de Riesgos

Se establece las acciones estratégicas, técnicas y organizacionales orientadas a reducir la probabilidad e impacto de los riesgos identificados en el Mapa de Riesgos de TI y en el Mapa de Riesgos Institucionales.

Objetivo del plan

Definir e implementar medidas preventivas, predictivas y correctivas que permitan mitigar los riesgos que afectan los activos de información y garantizar la continuidad de los servicios críticos de la entidad.

Estrategias de tratamiento

- Mitigación: aplicar controles de seguridad que reduzcan la probabilidad o impacto de los riesgos (ej. parches de seguridad, autenticación multifactor, segmentación de redes, cifrado de información).
- Transferencia: trasladar la gestión del riesgo a un tercero mediante seguros, contratos tecnológicos o acuerdos de niveles de servicio (SLA).
- Aceptación: reconocer riesgos con bajo impacto o baja probabilidad, documentando la justificación y el plan de monitoreo.
- Eliminación: suprimir el riesgo mediante la eliminación del activo, servicio o proceso que lo origina.

Acciones prioritarias

- Fortalecer la infraestructura tecnológica con herramientas de monitoreo centralizado (SIEM), análisis de vulnerabilidades y gestión de parches.
- Implementar y probar de forma periódica los planes de continuidad y recuperación (BCP/DRP), en cumplimiento con la ISO 22301:2019.
- Establecer cláusulas contractuales de seguridad y privacidad en todos los contratos de TI, garantizando la corresponsabilidad de proveedores.
- Consolidar campañas de cultura digital y capacitación obligatoria en seguridad de la información para funcionarios, contratistas y terceros.
- Documentar y mejorar el procedimiento de gestión de incidentes, con simulacros anuales y protocolos de comunicación institucional.

Responsables de la implementación

- El Coordinador TI lidera la definición, ejecución y actualización del plan.
- La Mesa de Ayuda (MDA) ejecuta acciones operativas de mitigación y soporte.
- El Comité de Gestión y Desempeño Institucional valida los avances y aprueba acciones estratégicas adicionales.
- Control Interno supervisa la efectividad del plan y emite recomendaciones.

Seguimiento y actualización

El plan será evaluado trimestralmente, con cortes en abril, agosto y diciembre, consolidando informes de avance y soportes documentales. Los resultados de cada ciclo alimentarán la revisión anual del MSPI, los reportes al FURAG y los informes de control interno.

Este plan asegura que los riesgos no solo sean identificados y valorados, sino también gestionados de forma efectiva, garantizando resiliencia institucional y confianza en los servicios de EPC.

Directrices Generales del MSPI

La implementación del Modelo se rige por un conjunto de directrices que orientan la gestión institucional, garantizando la protección de la información y la sostenibilidad de los procesos digitales, estas directrices se fundamentan en la normatividad nacional, los lineamientos del MinTIC y los estándares internacionales adoptados.

Gestión integral de activos de información

- Mantener actualizado el inventario de activos de información, asegurando su clasificación según criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
- Asignar responsables para cada activo y garantizar controles proporcionales a su nivel de criticidad.

Seguridad en infraestructura tecnológica y servicios críticos

- Proteger las infraestructuras críticas cibernéticas mediante esquemas de redundancia, segmentación de redes, sistemas de respaldo y pruebas periódicas de recuperación.
- Implementar controles de seguridad en la operación de servidores, redes, bases de datos, aplicaciones y servicios en la nube.

Gestión de accesos y control de usuarios

- Definir políticas claras de acceso basadas en el principio de mínimo privilegio.
- Implementar mecanismos de autenticación multifactor (MFA) y trazabilidad de auditoría en las cuentas críticas.

Relación con proveedores y servicios en la nube

- Incluir cláusulas de seguridad digital en los contratos de prestación de servicios tecnológicos.
- Supervisar el cumplimiento de los proveedores en materia de confidencialidad, continuidad y niveles de servicio (SLA).
- Adoptar lineamientos de ISO/IEC 27017 y ISO/IEC 27018 para servicios en la nube.

Prevención y gestión de incidentes

- Establecer un procedimiento formal de detección, reporte, análisis, atención y cierre de incidentes de seguridad de la información.
- Realizar simulacros anuales de incidentes y pruebas de respuesta a ciberataques.

Protección de datos personales y privacidad

- Cumplir de manera estricta la Ley 1581 de 2012 y sus decretos reglamentarios.
- Implementar medidas de anonimización, control de autorizaciones y auditorías de privacidad.
- Garantizar los derechos de los titulares frente al tratamiento de sus datos.

Capacitación y cultura organizacional en seguridad digital

- Incluir la seguridad digital en los procesos de inducción, reinducción y capacitaciones anuales.
- Ejecutar campañas de sensibilización y divulgar alertas sobre riesgos de ciberseguridad.

Monitoreo, auditoría y mejora continua

- Integrar la seguridad digital al ciclo PHVA (Planear, Hacer, Verificar y Actuar).
- Monitorear la infraestructura tecnológica mediante plataformas centralizadas de gestión de eventos de seguridad (SIEM).
- Incorporar hallazgos de auditorías internas, de control interno y de entes externos como insumos de mejora continua.

Transparencia y servicios ciudadanos digitales

- Asegurar que la provisión de información pública y de servicios digitales cumpla los lineamientos de la Política de Gobierno Digital y la Ley 1712 de 2014.
- Garantizar la confianza de los ciudadanos en los sistemas y trámites institucionales.

Sostenibilidad digital

- Promover el uso eficiente de recursos tecnológicos, la disposición adecuada de residuos electrónicos (RAEE), la reducción del consumo de papel y el teletrabajo.
- Alinear la gestión de la seguridad digital con los Objetivos de Desarrollo Sostenible (ODS) y las políticas ambientales de la entidad.

Estas directrices constituyen la base para el despliegue del MSPI, asegurando que la seguridad digital sea un eje transversal en todos los niveles de la gestión institucional.

Roles y Responsabilidades

La implementación requiere la participación coordinada de diferentes actores institucionales, con responsabilidades claramente definidas para garantizar la efectividad del sistema.

Coordinador de Tecnologías de la Información (Coordinador TI)

- Liderar la implementación, mantenimiento y mejora del MSPI.
- Coordinar el diseño y aplicación de políticas, procedimientos y controles de seguridad digital.
- Administrar el inventario de activos de información y asegurar su protección.
- Presentar informes de gestión de riesgos, incidentes y madurez al Comité de Gestión y Desempeño Institucional.
- Asegurar la inclusión de cláusulas de seguridad en los contratos tecnológicos.

Mesa de Ayuda (MDA)

- Ejecutar operativamente los controles definidos en el MSPI.
- Administrar accesos, respaldos, actualizaciones y monitoreo de sistemas.
- Registrar, clasificar y escalar incidentes de seguridad digital.
- Apoyar la actualización del inventario de activos de información.

Comité de Gestión y Desempeño Institucional

- Aprobar el MSPI y sus actualizaciones.
- Revisar periódicamente los resultados del autodiagnóstico MSPI, auditorías y seguimientos de riesgos.
- Definir acciones estratégicas frente a incidentes o riesgos de alto impacto.
- Garantizar la articulación del MSPI con el MIPG y la planeación institucional.

Dirección de Planeación

- Asegurar que el MSPI se integre en el Plan Estratégico Institucional (PEI) y en el PETI.
- Incorporar metas de seguridad digital en los planes de acción institucionales.

Equipo de Gestión de Calidad

- Verificar la coherencia del MSPI con el Sistema Integrado de Gestión.
- Coordinar la publicación de actualizaciones en los canales institucionales.

Oficina de Control Interno

- Realizar auditorías y evaluaciones independientes sobre la efectividad del MSPI.
- Emitir recomendaciones de mejora y verificar su implementación.

Áreas de apoyo transversales

- Jurídica: incluir y supervisar cláusulas de seguridad digital en la contratación pública.
- Talento Humano: garantizar la formación en seguridad digital dentro de la inducción, reinducción y capacitación anual.
- Proveedores y contratistas tecnológicos: cumplir las cláusulas contractuales relacionadas con seguridad, confidencialidad y continuidad del servicio.

Usuarios institucionales

Todos los funcionarios, contratistas y terceros que accedan a los activos de información son responsables de cumplir con las políticas del MSPI, aplicar buenas prácticas en seguridad digital y reportar incidentes de forma inmediata.

Gobernanza y tres líneas de defensa

La gobernanza del Modelo de Seguridad y Privacidad de la Información (MSPI) en EPC se estructura bajo el esquema de las tres líneas de defensa definido en el Modelo Integrado de Planeación y Gestión (MIPG), el cual asegura independencia, trazabilidad y eficacia en la gestión de los riesgos de seguridad digital.

- **Primera línea de defensa**: está conformada por el Coordinador de Tecnologías de la Información (TI) y la Mesa de Ayuda (MDA), son responsables de la ejecución operativa del MSPI, la implementación de controles técnicos y administrativos, la gestión de incidentes, la administración de accesos y la atención a usuarios. Esta línea responde directamente por la eficacia de los controles aplicados en el día a día.

- **Segunda línea de defensa**: corresponde a las áreas de Planeación Estratégica, Oficina Jurídica y Gestión de Calidad, que cumplen funciones de supervisión, orientación normativa y monitoreo del cumplimiento de políticas. Aseguran que los riesgos de seguridad sean gestionados de acuerdo con la normativa vigente y que las decisiones de TI estén alineadas con el PEI, PETI y PESI.
- **Tercera línea de defensa**: está a cargo de la Oficina de Control Interno, que brinda aseguramiento independiente y objetivo sobre la eficacia del MSPI, revisando la implementación de controles, el cumplimiento normativo y la efectividad del sistema de gestión en su conjunto, sus reportes alimentan los procesos de mejora continua y la rendición de cuentas institucional.

Con este esquema, EPC garantiza que la seguridad y privacidad de la información no sea solo una responsabilidad técnica, sino un componente de gobernanza que articula los niveles operativos, estratégicos y de control, fortaleciendo la transparencia y la confianza ciudadana.

Relación con Proveedores y Servicios en la Nube

La gestión de la seguridad digital incluye la supervisión y control de los proveedores que prestan servicios tecnológicos, así como la adopción de lineamientos para el uso seguro de servicios en la nube.

Relación con proveedores tecnológicos

- Todos los contratos que involucren el suministro de bienes o servicios de TI deberán incluir cláusulas de seguridad digital, que contemplen:
  - Confidencialidad y protección de la información institucional.
  - Cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.
  - Garantía de continuidad de los servicios mediante planes de contingencia.
  - Inclusión de acuerdos de nivel de servicio (SLA) que especifiquen tiempos de respuesta, disponibilidad y métricas de calidad.
- Los proveedores deberán reportar incidentes de seguridad que afecten los activos de información de EPC y colaborar en su investigación y resolución.
- El incumplimiento de las obligaciones contractuales podrá dar lugar a sanciones, según lo estipulado en la ley.

Servicios en la nube

El uso de servicios en la nube por parte de EPC deberá realizarse bajo un marco de seguridad basado en estándares internacionales y lineamientos del MinTIC:

- Aplicación de controles de la ISO/IEC 27017 (seguridad en servicios de nube) y de la ISO/IEC 27018 (protección de datos personales en la nube).
- Evaluación de proveedores bajo criterios de seguridad, disponibilidad, localización de datos y cumplimiento normativo.
- Garantía contractual sobre la propiedad de la información institucional y el acceso exclusivo por parte de EPC.
- Establecimiento de procedimientos de respaldo, portabilidad y recuperación de datos en caso de terminación del servicio o contingencia.
- Monitoreo continuo del cumplimiento de proveedores mediante revisiones periódicas, auditorías o certificaciones de seguridad (ISO 27001, SOC 2, entre otras).

Supervisión y trazabilidad

- Los informes de supervisión a proveedores deberán documentarse y presentarse al Comité de Gestión y Desempeño Institucional.
- Toda la información generada en la relación con proveedores y servicios en la nube será registrada en los repositorios institucionales para garantizar trazabilidad y facilitar auditorías internas y externas.

La adecuada gestión de proveedores y el uso seguro de servicios en la nube permiten a EPC fortalecer su capacidad de resiliencia, asegurar la continuidad de

los servicios digitales y garantizar la confianza ciudadana en la administración de sus datos.

Gestión de Incidentes de Seguridad de la Información

La gestión de incidentes de seguridad es un componente esencial orientado a garantizar la detección, registro, análisis, atención y cierre de eventos que afecten o puedan afectar la seguridad y privacidad de la información.

Definición de incidente

Se considera incidente de seguridad de la información cualquier evento que comprometa o intente comprometer la confidencialidad, integridad, disponibilidad o privacidad (CIDP) de los activos de información, esto incluye accesos no autorizados, pérdida o robo de información, ataques cibernéticos, malware, interrupciones de servicios críticos, fallas en infraestructura tecnológica o filtraciones de datos personales.

Ciclo de gestión de incidentes

- Detección y reporte: todos los funcionarios, contratistas y proveedores tienen la obligación de reportar incidentes de seguridad al Coordinador TI o a la Mesa de Ayuda (MDA), mediante los canales establecidos (correo institucional, sistema de tickets, línea de atención o formato oficial).
- Registro y clasificación: la MDA documenta el incidente, asigna un nivel de criticidad (alto, medio o bajo) y relaciona los activos comprometidos.
- Análisis e investigación: el Coordinador TI evalúa la causa raíz, el alcance y las posibles consecuencias, definiendo las acciones inmediatas de contención.
- Respuesta y mitigación: se aplican controles correctivos y medidas técnicas para restaurar los servicios, proteger los datos y evitar la propagación del incidente.
- Cierre y documentación: una vez solucionado, se genera un informe con la descripción del incidente, acciones aplicadas, tiempos de respuesta y resultados obtenidos.
- Retroalimentación y mejora: los aprendizajes derivados se incorporan al Plan de Tratamiento de Riesgos, al PESI y a los procedimientos de seguridad, fortaleciendo la capacidad de respuesta institucional.

Responsabilidades

- El Coordinador TI lidera el proceso, coordina las respuestas y reporta los incidentes críticos al Comité de Gestión y Desempeño Institucional.
- La MDA ejecuta la atención operativa, mantiene registros actualizados y comunica los incidentes a los responsables designados.
- Los usuarios institucionales deben reportar inmediatamente cualquier anomalía o sospecha de incidente.
- Control Interno podrá verificar la gestión de incidentes como parte de las auditorías internas.

Simulacros y pruebas

EPC realizará simulacros anuales de incidentes y pruebas de ciberseguridad, evaluando la capacidad de detección, respuesta y recuperación, los resultados serán documentados e incorporados en la mejora continua del MSPI, la gestión estructurada de incidentes garantiza que EPC pueda anticipar, responder y aprender de los eventos de seguridad, fortaleciendo la resiliencia institucional y la confianza de los ciudadanos en la prestación de los servicios públicos.

Continuidad de Negocio y Recuperación ante Desastres

La continuidad de negocio y la recuperación ante desastres son componentes fundamentales del MSPI en Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), cuyo propósito es garantizar que los procesos críticos y los servicios esenciales de la entidad se mantengan operativos o se restablezcan en tiempos aceptables ante la ocurrencia de incidentes graves o desastres.

Lineamientos de continuidad de negocio

- Identificar los procesos críticos y los servicios esenciales de la entidad, priorizando aquellos relacionados con la prestación de servicios públicos domiciliarios y la atención a los ciudadanos.
- Establecer análisis de impacto en el negocio (BIA – Business Impact Analysis) que determine las dependencias tecnológicas, los tiempos máximos de recuperación (RTO) y los niveles mínimos de servicio aceptables.
- Diseñar y mantener actualizado el Plan de Continuidad de Negocio (BCP), alineado con la ISO 22301:2019 y la normatividad nacional vigente.
- Definir estrategias de redundancia tecnológica, respaldo de información, replicación de datos y disponibilidad de recursos alternos que permitan mantener la operación en caso de interrupción.

Lineamientos de recuperación ante desastres

- Implementar un Plan de Recuperación ante Desastres (DRP) que contemple la restauración de infraestructura tecnológica, aplicaciones, bases de datos y servicios en la nube.
- Establecer mecanismos de respaldo periódico, pruebas de restauración y verificación de la integridad de la información respaldada.
- Definir un sitio alterno o estrategias de continuidad en la nube que garanticen la disponibilidad de los servicios críticos en caso de afectación de los centros de datos principales.
- Incorporar protocolos de comunicación interna y externa para informar oportunamente a las partes interesadas sobre el estado de los servicios durante una contingencia.

Pruebas y simulacros

- Realizar pruebas de continuidad de negocio y simulacros de recuperación al menos una vez al año, documentando los resultados y lecciones aprendidas.
- Ajustar los planes (BCP y DRP) con base en los hallazgos identificados en las pruebas y auditorías internas.

Responsables

- El Coordinador TI lidera la definición, actualización y activación de los planes de continuidad y recuperación.
- La Mesa de Ayuda (MDA) ejecuta operativamente los procedimientos de respaldo, restauración y soporte técnico durante las contingencias.
- El Comité de Gestión y Desempeño Institucional aprueba los planes y hace seguimiento a su efectividad.

La gestión de continuidad de negocio y recuperación ante desastres asegura que EPC pueda responder de manera organizada y efectiva a eventos disruptivos, reduciendo impactos en la operación institucional y manteniendo la confianza de los ciudadanos en la prestación de sus servicios.

Sostenibilidad digital y gestión ambiental de TIC

La gestión de la seguridad y privacidad de la información en EPC se desarrolla bajo un enfoque de sostenibilidad digital, que reconoce la necesidad de reducir la huella ambiental de las Tecnologías de la Información y las Comunicaciones (TIC), este

enfoque responde a las políticas nacionales de sostenibilidad, los compromisos de mitigación del cambio climático y las orientaciones del FURAG.

Las acciones institucionales en esta materia incluyen:

- Gestión responsable de residuos de aparatos eléctricos y electrónicos (RAEE): EPC implementa procedimientos para la disposición final de equipos de cómputo, periféricos y dispositivos tecnológicos, conforme a la normatividad ambiental vigente.
- Eficiencia energética: se promueve el uso de tecnologías de bajo consumo energético, la virtualización de servidores y el empleo de soluciones en la nube que reduzcan la huella de carbono.
- Optimización de recursos digitales: migración hacia trámites electrónicos, uso de firma digital, implementación de workflows sin papel y almacenamiento digital eficiente.
- Compras sostenibles en TIC: inclusión de criterios ambientales en la adquisición de equipos y servicios tecnológicos, privilegiando aquellos con certificaciones de eficiencia y sostenibilidad.
- Capacitación y cultura ambiental digital: programas de sensibilización para funcionarios y contratistas en el uso racional de los recursos tecnológicos y en el adecuado manejo de equipos obsoletos.

Con estas medidas, EPC asegura que la gestión de TIC no solo fortalezca la seguridad de la información, sino que también contribuya a la responsabilidad ambiental institucional, alineando la seguridad digital con la sostenibilidad y los Objetivos de Desarrollo Sostenible (ODS).

Protección de Datos Personales y Privacidad

El tratamiento de los datos personales se realiza bajo un enfoque de respeto a los derechos fundamentales de los titulares de la información, en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013, la Ley 1712 de 2014 de transparencia y acceso a la información, así como las directrices emitidas por la Superintendencia de Industria y Comercio (SIC) y las recomendaciones del MinTIC en materia de seguridad digital, adicionalmente, EPC adopta las buenas prácticas de protección de datos personales definidas en la ISO/IEC 29100 y en la ISO/IEC 27701 sobre gestión de privacidad.

Principios rectores del tratamiento de datos personales: El tratamiento de la información personal en EPC se rige por los siguientes principios:

- Legalidad: todo tratamiento de datos se fundamenta en lo establecido en la normatividad vigente.
- Finalidad: los datos se recolectan y tratan únicamente para fines legítimos, explícitos y previamente informados a los titulares.
- Libertad: el tratamiento requiere autorización previa, expresa e informada del titular.
- Veracidad o calidad: la información debe ser veraz, completa, exacta, actualizada y verificable.
- Transparencia: se garantiza el derecho de los titulares a conocer, actualizar y rectificar su información.
- Acceso y circulación restringida: el acceso a los datos personales está limitado exclusivamente a personas autorizadas y con fines legítimos.
- Seguridad: se implementan medidas técnicas, administrativas y jurídicas para prevenir pérdida, acceso no autorizado, alteración indebida o divulgación no autorizada.
- Confidencialidad: todos los funcionarios, contratistas y terceros involucrados en el tratamiento están obligados a garantizar la reserva de la información.
- Responsabilidad demostrada (accountability): EPC documenta y evidencia la adopción de medidas para garantizar la protección efectiva de los datos personales.

Medidas implementadas en EPC: Para garantizar la protección de los datos personales, la entidad implementa las siguientes medidas:

- Políticas y procedimientos internos que regulan el tratamiento de datos personales, disponibles para consulta ciudadana.
- Registro y actualización de las bases de datos ante la Superintendencia de Industria y Comercio (SIC), en cumplimiento del Régimen de Protección de Datos Personales.
- Inclusión de cláusulas contractuales de privacidad y protección de datos en los acuerdos con proveedores, contratistas y aliados estratégicos.
- Aplicación de medidas técnicas como control de accesos, autenticación multifactor, cifrado de datos sensibles, copias de seguridad cifradas y registros de auditoría.
- Procedimientos para la atención de consultas, peticiones, quejas y reclamos (Habeas Data) de los titulares, garantizando oportunidad y trazabilidad.

- Protocolos de gestión de incidentes relacionados con filtración, pérdida, robo o uso indebido de datos personales, incluyendo planes de notificación a la SIC y a los titulares afectados.
- Incorporación del principio de privacidad desde el diseño (Privacy by Design) en el desarrollo e implementación de nuevos sistemas de información.

Derechos de los titulares: todo ciudadano cuyos datos sean tratados por EPC tiene derecho a:

- Acceder a su información personal y conocer el uso que se le está dando.
- Solicitar la actualización, corrección o supresión de sus datos cuando sean incompletos, inexactos o ya no sean necesarios para la finalidad autorizada.
- Revocar la autorización otorgada para el tratamiento, en los casos previstos por la ley.
- Presentar quejas ante la SIC en caso de vulneración de sus derechos.
- Responsabilidades institucionales
- El Coordinador TI asegura la implementación de medidas técnicas y operativas para la protección de datos personales, garantizando que los sistemas y servicios cumplan con criterios de seguridad y privacidad.
- La Oficina Asesora Jurídica garantiza la conformidad legal de los procedimientos y responde a consultas, requerimientos de la SIC y solicitudes de los titulares.
- El Equipo de Gestión de Calidad asegura la integración de la gestión de datos personales al Sistema Integrado de Gestión y al MIPG.
- La Mesa de Ayuda (MDA) apoya con la administración de incidentes y la evidencia operativa de cumplimiento de controles.
- Todos los funcionarios, contratistas y terceros deben cumplir las disposiciones sobre privacidad, aplicando buenas prácticas en el manejo de la información personal.

Servicios Ciudadanos Digitales y Transparencia

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) se articula con la Política de Gobierno Digital, regulada por el Decreto 338 de 2022, que impulsa la provisión de trámites y servicios en línea bajo condiciones de seguridad, eficiencia, accesibilidad e interoperabilidad, garantizando que los ciudadanos cuenten con servicios confiables y que la gestión pública avance en la consolidación de un ecosistema digital transparente y seguro.

Servicios Ciudadanos Digitales

EPC adopta las directrices del MinTIC para la implementación de los Servicios Ciudadanos Digitales, asegurando que:

- El acceso a los trámites y servicios digitales se realice bajo condiciones de confidencialidad, integridad, disponibilidad y privacidad, en cumplimiento de lo establecido en el MSPI.
- Se empleen mecanismos de autenticación digital confiable, autenticación multifactor y otros esquemas seguros definidos por el Estado colombiano.
- Se garantiza interoperabilidad de los sistemas de información con plataformas del Estado, en cumplimiento de los lineamientos de arquitectura empresarial, gobierno de datos y estándares abiertos.
- Se incluyen controles técnicos de seguridad para proteger la integridad, disponibilidad y trazabilidad de los datos intercambiados en transacciones electrónicas.

Transparencia y acceso a la información pública

En cumplimiento de la Ley 1712 de 2014 sobre transparencia y acceso a la información, EPC asegura la publicación proactiva, accesible y actualizada de información pública en su portal institucional, incluyendo:

- Políticas, planes, informes de gestión, normatividad aplicable, resultados de auditorías y procesos de contratación.
- Información disponible en formatos abiertos y reutilizables, que favorezcan la participación ciudadana, la innovación y el control social.
- Contenidos con mecanismos de seguridad que protejan la integridad y disponibilidad de la información publicada.
- Evidencia y trazabilidad de los procesos de publicación, actualización y custodia de la información institucional.
- Protección en los servicios digitales
- Los sistemas que soportan trámites y servicios en línea deben cumplir con los controles exigidos por el MSPI, la ISO/IEC 27001, y los lineamientos de la ISO/IEC 27017 y 27018 cuando utilicen servicios en la nube.
- Se implementan procesos de auditoría, monitoreo y registro de eventos para prevenir, detectar y responder a accesos indebidos, intentos de fraude o alteraciones de la información en los servicios digitales.
- Los planes de continuidad y recuperación ante incidentes se extienden a los trámites y servicios ciudadanos digitales, garantizando su disponibilidad en situaciones críticas.

Capacitación y Cultura Organizacional en Seguridad Digital

El fortalecimiento de la cultura de seguridad digital es un componente transversal del MSPI, que busca garantizar que funcionarios, contratistas y proveedores comprendan la importancia de proteger la información y apliquen buenas prácticas en su manejo.

Programas de capacitación

- Todos los funcionarios y contratistas deben recibir capacitación obligatoria en seguridad digital como parte de los procesos de inducción, reinducción y formación anual.
- Los proveedores y terceros que presten servicios tecnológicos deberán acreditar programas de formación para su personal, como requisito contractual.
- Los contenidos estarán orientados a:
    - Principios de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
    - Buenas prácticas en el uso de contraseñas, correo electrónico, navegación web y dispositivos móviles.
    - Procedimientos de reporte de incidentes de seguridad.
    - Cumplimiento de la Ley 1581 de 2012, la Ley 1712 de 2014 y la Ley 1273 de 2009.
    - Lineamientos de seguridad en servicios en la nube y protección de datos personales.

Cultura organizacional en seguridad digital

- Ejecución de campañas periódicas de sensibilización sobre ciberseguridad y privacidad.
- Difusión de boletines internos y alertas de seguridad en los canales institucionales.
- Inclusión de la seguridad digital en la agenda del Comité de Gestión y Desempeño Institucional.
- Promoción del uso responsable de las tecnologías, la reducción del consumo de papel, el teletrabajo y la disposición adecuada de residuos electrónicos (RAEE).
- Reconocimiento a funcionarios o equipos que demuestren compromiso y buenas prácticas en la gestión de la seguridad de la información.

Responsabilidades

- El Coordinador TI define el programa anual de capacitación y coordina su ejecución con la Oficina de Talento Humano.
- La Mesa de Ayuda (MDA) participa en la difusión de alertas y en el acompañamiento a los usuarios en el uso seguro de herramientas digitales.
- Todos los usuarios institucionales son responsables de aplicar los conocimientos adquiridos y de contribuir activamente a la cultura de seguridad digital.

La capacitación y la sensibilización continua fortalecen la capacidad de EPC para reducir incidentes originados por errores humanos, asegurar el cumplimiento normativo y garantizar la apropiación del MSPI en todos los niveles de la entidad.

Indicadores de Seguimiento y Evaluación

El cumplimiento y efectividad será evaluado a través de un sistema de indicadores que permitan medir avances, resultados y oportunidades de mejora en materia de seguridad digital.

Indicadores estratégicos

- Porcentaje de implementación de acciones del MSPI frente al plan anual aprobado.
- Nivel de madurez alcanzado en el autodiagnóstico MSPI, comparado con el ciclo anterior.
- Grado de alineación del MSPI con el PETI, el PESI y el Plan Estratégico Institucional.

Indicadores de gestión operativa

- Porcentaje de activos de información inventariados y clasificados según criticidad.
- Porcentaje de incidentes de seguridad gestionados dentro de los tiempos establecidos.
- Tiempo promedio de detección y respuesta ante incidentes de seguridad.
- Porcentaje de proveedores tecnológicos supervisados con cumplimiento de cláusulas de seguridad.
- Porcentaje de sistemas críticos con respaldos verificados y pruebas exitosas de recuperación.
- Número de simulacros de continuidad de negocio y pruebas de recuperación ejecutados al año.

Indicadores de cultura organizacional y capacitación

- Porcentaje de funcionarios y contratistas capacitados en seguridad digital en inducción, reinducción y formación anual.
- Número de campañas de sensibilización en ciberseguridad realizadas anualmente.
- Nivel de participación de los usuarios en actividades de cultura de seguridad digital.

Fuentes de información

Los indicadores se alimentarán de registros de la Mesa de Ayuda (MDA), informes del Coordinador TI, resultados del autodiagnóstico MSPI, auditorías internas, reportes de proveedores y seguimiento del Comité de Gestión y Desempeño Institucional.

Seguimiento y reporte

- El seguimiento será anual.
- Los resultados se presentarán al Comité de Gestión y Desempeño Institucional y se reportarán en el FURAG, en cumplimiento del MIPG.
- Los indicadores servirán como base para la revisión anual del MSPI y para la adopción de acciones de mejora continua.

Con este sistema de indicadores, EPC asegura la trazabilidad, objetividad y sostenibilidad en la gestión de la seguridad digital, garantizando un monitoreo efectivo y la alineación con las políticas nacionales e internacionales.

Seguimiento, Articulación con Auditorías Internas y Externas, e Indicadores de Evaluación

El seguimiento al MSPI es un componente esencial para garantizar su efectividad y su mejora continua, este se articula con los procesos de auditoría, control interno y reporte institucional, asegurando trazabilidad en la gestión de la seguridad de la información.

Mecanismos de seguimiento y auditoría

- Autodiagnóstico MSPI: aplicación anual y extraordinaria según lineamientos del MinTIC, que mide el nivel de madurez de la entidad en seguridad digital.

- Auditorías internas: revisiones periódicas realizadas por Control Interno para verificar el cumplimiento de políticas, controles y procedimientos del MSPI.
- Auditorías externas y de entes de control: incluyen la Revisoría Fiscal, la Superintendencia de Servicios Públicos, la SIC y demás organismos de supervisión, que validan el cumplimiento normativo y contractual.
- FURAG (Formulario Único de Reporte de Avances de la Gestión): reporte oficial ante el DAFP que incluye resultados de Gobierno Digital y Seguridad de la Información.
- Revisión por la dirección: análisis y toma de decisiones en el Comité de Gestión y Desempeño Institucional, con base en indicadores y resultados de auditorías.

Indicadores de evaluación

Los indicadores permiten medir el grado de implementación, efectividad y mejora del MSPI. Entre ellos se destacan:

- Porcentaje de implementación de acciones del PESI y del MSPI.
- Nivel de madurez alcanzado en el autodiagnóstico MSPI frente al ciclo anterior.
- Porcentaje de incidentes de seguridad atendidos dentro de los tiempos establecidos.
- Tiempo promedio de detección y respuesta a incidentes.
- Porcentaje de activos de información clasificados y protegidos con controles aplicados.
- Porcentaje de proveedores con cláusulas de seguridad y continuidad en sus contratos.
- Porcentaje de acciones de mejora implementadas derivadas de auditorías internas, externas y del FURAG.
- Porcentaje de dispositivos tecnológicos gestionados conforme a la normatividad ambiental (RAEE).

Responsables

- El Coordinador TI consolida resultados de indicadores y auditorías, y presenta informes a la dirección.
- La Mesa de Ayuda (MDA) aporta evidencia operativa y registros de incidentes.
- El Equipo de Gestión de Calidad asegura la integración de los resultados al Sistema Integrado de Gestión.
- La Oficina de Control Interno garantiza independencia y asegura que las recomendaciones sean implementadas en los ciclos de mejora.

Con este esquema, el MSPI no solo se convierte en un sistema de gestión de seguridad digital, sino en un modelo de gobernanza verificable y auditable, alineado con las mejores prácticas internacionales y con los compromisos de transparencia de la gestión pública.

Verificación, Revisión y Actualización del MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) es un instrumento dinámico que debe ser verificado, revisado y actualizado de manera periódica y extraordinaria, asegurando su vigencia, pertinencia y efectividad frente a los cambios normativos, tecnológicos y organizacionales.

Periodicidad ordinaria

- El MSPI será revisado y actualizado anualmente, en coherencia con el ciclo de planeación institucional y los resultados del autodiagnóstico MSPI.
- La verificación incluirá la evaluación de indicadores, el cumplimiento de controles y los avances del Plan de Tratamiento de Riesgos.

Circunstancias extraordinarias de actualización

La revisión podrá realizarse en cualquier momento cuando se presenten:

- Cambios relevantes en la normatividad nacional o en los lineamientos del MinTIC.
- Incidentes de seguridad críticos que comprometan activos de información o servicios institucionales.
- Transformaciones tecnológicas significativas, como migraciones de sistemas a la nube o implementación de nuevas infraestructuras críticas.
- Recomendaciones derivadas de auditorías internas, control interno, entes de control o revisiones de la dirección.

Responsables de la verificación y revisión

- El Coordinador TI lidera el proceso de revisión, proponiendo los ajustes necesarios.
- La Mesa de Ayuda (MDA) suministra información operativa sobre incidentes, controles aplicados y gestión de activos.
- El Comité de Gestión y Desempeño Institucional aprueba las actualizaciones y asegura la integración del MSPI en la planeación estratégica.

- El Equipo de Gestión de Calidad valida la coherencia con el Sistema Integrado de Gestión y coordina la publicación de las actualizaciones en los canales oficiales.
- Oficina de Control Interno garantiza independencia en la verificación y emite recomendaciones de mejora.

Articulación con la mejora continua

El proceso de revisión del MSPI se integra al ciclo PHVA (Planear, Hacer, Verificar, Actuar), asegurando que los resultados de indicadores, auditorías, autodiagnósticos y evaluaciones externas se traduzcan en acciones concretas de mejora, fe esta manera, EPC asegura que su MSPI evolucione de manera permanente, respondiendo a los retos emergentes en materia de ciberseguridad y fortaleciendo la confianza ciudadana en la gestión de la entidad.

Disposiciones Finales

El Modelo de Seguridad y Privacidad de la Información (MSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) es de cumplimiento obligatorio para todos los funcionarios, contratistas, proveedores y terceros que gestionen o accedan a los activos de información institucional, su aplicación busca fortalecer la resiliencia digital de la entidad, garantizar la continuidad de los servicios públicos y proteger los derechos de los ciudadanos en materia de datos personales y transparencia.

La responsabilidad de coordinar la implementación, seguimiento y mejora continua del MSPI recae en el Coordinador TI, con apoyo operativo de la Mesa de Ayuda (MDA), el Comité de Gestión y Desempeño Institucional será la instancia encargada de aprobar actualizaciones, revisar avances y definir acciones estratégicas frente a riesgos o incidentes críticos.

El presente modelo será publicado en la página web institucional y en los canales oficiales de EPC, en cumplimiento de la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública, asimismo, se incorporará como parte integral del Sistema Integrado de Gestión de la entidad.

El incumplimiento de las disposiciones establecidas en este modelo podrá dar lugar a medidas administrativas, disciplinarias, contractuales o legales, según lo determine la normatividad vigente y la gravedad de la falta.

Con la adopción del MSPI, EPC reafirma su compromiso con:

- La protección de la información institucional y los datos personales de los ciudadanos.
- El cumplimiento de la normatividad colombiana en materia de seguridad digital.
- La aplicación de estándares internacionales reconocidos en ciberseguridad y gestión de riesgos.
- La consolidación de una cultura organizacional de seguridad, transparencia y sostenibilidad digital.

Estas disposiciones finales aseguran que el MSPI no solo sea un documento de referencia, sino un instrumento vivo, dinámico y transversal, que guía la gestión de la seguridad digital en EPC con un enfoque de mejora continua y confianza ciudadana.